

SECURE ENCRYPTION OF DATA PACKETS FOR TRANSMISSION OVER
UNSECURED NETWORKS

JULY 1997

B>

BACKGROUND OF THE INVENTION

1. Technical Field:

5 The present invention relates in general to data encryption and in particular to securing data transfers over unsecured channels of communications. Still more particularly, the present invention relates to practical implementation of unbreakable data encryption through one-time use of pure random numbers.

2. Description of the Related Art:

20 Sensitive data transfers are increasingly occurring over networks which are unsecured, such as the Internet or cellular telephone networks. By their nature, the medium by which data transfers are made in such networks must be openly accessible and/or shared, leaving transactions susceptible to interception. The only available alternative for securing data transfers over such networks thus becomes data encryption.

25 A variety of data encryption schemes have been developed and are implemented for data transfers over networks of the type described. For example, many data encoding schemes employ a reversible encryption algorithm modeled after the Data Encryption Standard (DES). Other data encoding schemes, used alone or in conjunction with DES, employ a combination of public and private keys to encrypt data, such as the Rivest-Shamir-Aldeman (RSA) encryption system used in many commercial software packages. These encoding schemes utilize pseudo-

random numbers, or number sequences having a high degree of randomness.

5 The only encryption system currently recognized as being unconditionally secure is the "one-time pad," also known as a Vernam cipher, developed by Gilbert S. Vernam while working for AT&T in 1917. When properly implemented, the one-time pad encryption mechanism is generally recognized by cryptographic experts to be the only known unbreakable encoding scheme.
10 Other encryption systems are considered cryptographically secure, meaning that the costs associated with breaking the code by pure mathematical methods and extensive computation are very high, although the code can theoretically be broken if enough computing power could be brought to bear. One-time pads are unconditionally secure, meaning that any amount of analysis and computing power is insufficient because there is no pattern in the data.

20 The two key characteristics of the one-time pad concept which must be adhered to for encryption with a one-time pad to be unconditionally secure are pure randomness and one-time use. Pure randomness is thought to occur in the timing of radioactive decay and in the arrival of cosmic background radiation. The present invention employs one or both of the above sources passed through a cryptographically strong one-way function as the source of random values. Furthermore, the present invention requires that the random sequences thus generated are never intentionally used in more than one embodiment.

25 30 Although recognized as being mathematically unbreakable, the one time pad is conventionally considered not to be

5

10

00000000000000000000000000000000

25

commercially practical. The reason is principally convenience, since the security of the system requires that the contents of the one-time pad be known only to the proper encrypting and decrypting entities. This requires secure distribution of the one-time pads. Furthermore, the one-time pad, when properly employed, requires large amounts of pure random data for the encryption/decryption values which, by definition, may be used only once. Additionally, since the one-time pad contains only a finite number of random numbers for encryption, replacement of the one-time pad is inevitably required. Finally, the one-time pad encryption method is less ideally suited for encryption of long, variable length messages than alternative, less secure encryption schemes. For these reasons, one-time pads have not been employed up to this time in actual encryption systems for commercial applications, such as banking, cellular telephony, etc.

There do exist classes of problems, however, for which the one-time pad could provide unconditionally secure encryption on a commercial basis. It would be desirable, therefore, to provide a method and apparatus for employing one-time pads in commercial applications requiring encryption of data for transfer over unsecured networks. It would further be advantageous to provide an implementation of one-time pads which could be readily adapted to a variety of commercial data encryption requirements.

SUMMARY OF THE INVENTION

It is therefore one object of the present invention to provide an improved method and apparatus for data encryption.

5

It is another object of the present invention to provide an improved method and apparatus for securing data transfers over unsecured channels of communications.

10 It is yet another object of the present invention to provide practical implementation of unbreakable data encryption through one-time use of pure random numbers.

15 The foregoing objects are achieved as is now described. Pure random numbers from a sheet within a one-time pad are employed to encrypt the bytes of a source data packet and to order the encrypted bytes in a random order within the encrypted data packet. Pure random numbers fill remaining positions within the encrypted data packet. The resulting encrypted data packet is unconditionally secure (i.e., unbreakable). Sheets within the one-time pad are utilized only once, and the one-time pad is replaced when exhausted. For electronic checking applications, the one-time pad is distributed to the user stored in an electronic checkbook, with a copy retained by the bank. For cellular telephone applications, the one-time pad is stored in a replaceable memory chip within the mobile unit with a copy retained at a single, secured central computer. For client-server applications or applications involving sales over the Internet, the one-time pad may be provided to the user on a floppy disk or 20 CD-ROM, with a copy retained by the vendor.

25

30

The above as well as additional objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a block diagram of a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 2 is a diagram of the contents of a sheet within a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 3 depicts an example of data encryption utilizing a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 4 is a high level flowchart for a process of encrypting data in accordance with a preferred embodiment of the present invention;

Figure 5 depicts a high level flowchart for a process of decoding data in accordance with a preferred embodiment of the present invention;

Figure 6 is a diagram of an electronic checking environment in which secure encryption in accordance with a

preferred embodiment of the present invention may be implemented;

5 **Figure 7** depicts a data flow diagram for a process of utilizing electronic checks in accordance with a preferred embodiment of the present invention;

10 **Figure 8** is a block diagram of a cellular communications global transponder in which a preferred embodiment of the present invention may be implemented; and

Figure 9 depicts an Internet sales environment in which a preferred embodiment of the present invention may be implemented.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures, and in particular with reference to **Figure 1**, a block diagram of a one-time pad in accordance with a preferred embodiment of the present invention is depicted. One-time pad 102 is maintained in a memory, such as a read only memory (ROM) or a hard disk drive, and includes a plurality of sheets 104. Each sheet 104 contains a plurality of pure random numbers sufficient for encryption of a known, fixed length (N) data packet. Each sheet 104 is not intentionally used in the implementation of any other one-time pads such as one-time pad 102.

Referring to **Figure 2**, a diagram of the contents of a sheet within a one-time pad in accordance with a preferred embodiment of the present invention is illustrated. Each sheet 104 contains a string 202 of N pure randomly-ordered numbers in the range of 1 to N. Each sheet 104 also contains a plurality of corresponding arrays 204. Number string 202 is a non-repeating sequence of numbers within the predetermined range N corresponding to the number of characters or positions in the encrypted data packet. For example, if the encrypted data packet will have five hundred positions, the numerals 1 through 500 will be randomly ordered and placed in string 202. Individual numbers within string 202 are employed to identify the position for a corresponding byte of data in the encrypted data packet. For example, the first number 206 within string 202 designates the position within the encrypted data packet in which the first byte of source data will be placed after encryption.

Each individual number within string 202 has an

associated array within array set 204. Each array 208 contains a non-repeating sequence of random numbers comprising a character map to be employed for the character in the respective position. For the sake of simplicity and clarity of explanation, the exemplary embodiment depicts only the mapping for numeric characters 0-9 and a delimiter ("*"). However, the mapping may easily be extended to include alphabetic or text characters merely by increasing the size of arrays 204. The arrays 204 essentially comprise encryption instructions for data packets not exceeding the length of position string 202.

The characters or values within a character map array 208 for a given position are randomly generated subject only to the constraint that the same value may not appear twice in a given array. However, the same value may appear many times within different arrays in array set 204. In fact, 128 different characters can be encoded in each byte comprising map array 208. While the exemplary embodiment depicts only numerals less than 100 in arrays 204, any set of 128 unique characters may be employed to form the character maps, including alphanumeric characters and special characters (colons, hyphens, dashes, quotation marks, punctuation, etc.).

The fact that only 128 different characters can be represented within any one byte of array 208 creates a limitation on the encryption of double byte based text that occurs in Asian languages. However, the present invention is likely to find its widest commercial use in short, fixed length, numeric related applications such as electronic checking, position reporting, and client-server authentication and verification. Since the present invention is not intended

for widespread use in text encryption, the exemplary embodiment illustrates a single byte approach. However, those skilled in the art will quickly understand that the present invention can be extended to include double byte encoding.

5 As described, the character map values within each array
10 208 in array set 204 are random numbers, and the sequence of
15 numbers in string 202 is randomly ordered. Two sources of
20 "randomness" are thought to exist: the time period associated
25 with electronic emission/decay for a single radioactive
30 particle and the level of background radiation originating
35 from space. Methods for generating pure random numbers are
40 well-known in the art, and include measuring the random time
45 intervals associated with radioactive decay or cosmic
50 background radiation and passing these measurements through a
55 one-way hash function. These methods may be employed in known
60 manners for generating values for the character maps in arrays
65 204, for randomly ordering numbers within string 202, and for
70 filling the unused bytes of the encrypted data packet.

Referring again to Figure 1, the requirement that true random numbers be employed in sheets 104 within one-time pad 102 cannot be circumvented for convenience. Pseudo-random numbers, which are usually generated from a seed value using a hash function, are not acceptable substitutes since an estimate of the seed value may be employed to derive the hash function required to duplicate the resulting pattern. With a fairly accurate estimate of the seed value, the number of mathematical operations required to crack the encryption mechanism becomes workable. The vulnerability of pseudo-random numbers, even those believed to be cryptographically secure, has been demonstrated where the time and process id

have been used in the key of popular software security features.

One-time pad 102 may also include counter 106 identifying the next sheet 104 which may be utilized for encryption or decryption. Both the encrypting and decrypting entities are provided with identical copies of one-time pad 102 through a secure medium such as hand-delivery. As sheets 104 within one-time pad 102 are utilized, counter 106 is advanced to point to the next available sheet. When counter 106 contains a value exceeding the number of sheets 104 within one-time pad 102, one-time pad 102 is depleted and must be replaced.

The requirement that a given sheet 104 within one-time pad 102 be used only once and never be reused is critical. Reuse of sheets 104 within one-time pad 102 compromises the security of the resulting encrypted data packet. It is intended that data packets encrypted by the method provided in the present invention could be accompanied by the plain text of the source packet, and still be invulnerable to cryptographic attack. Reuse of sheets 104 would prohibit this level of unconditionally secure encryption.

With reference now to **Figure 3**, an example of data encryption utilizing a one-time pad in accordance with a preferred embodiment of the present invention is depicted. Source data packet 302 contains a string of characters comprising the message to be encrypted for transmission. Again, while the exemplary embodiment depicts only numeric characters and a delimiter, the process described may be readily applied to expanded character sets.

Furthermore, the order in which the pure random numbers are used from sheet 104 within a specific one-time pad 102 can be varied depending on a particular customer or implementation. The same encoding/decoding software is simply placed in the one-time pad device and the decoding computer. This allows for further security through the ability to physically secure the one-time pad and the encoding/decoding software separately. The ability to separate responsibilities is one key method used in the prevention of theft by inside employees. In the exemplary embodiment, one particular pattern is followed for illustrative purposes.

The encrypted data packet 304 contains positions for the encrypted bytes of source data packet 302, with five hundred positions depicted in the exemplary embodiment. The value of the first numeral in the position string of a sheet in the one-time pad is utilized to determine the position of the first encrypted byte. Utilizing the example depicted in **Figure 2**, the first encrypted byte of source data packet is to be placed in position 3. The value of the first byte within source data packet is looked up in the associated character map for position 3, and the encrypted value "92" is entered in encrypted data packet 304 at position 3. Similarly, the value "67" is entered in position 14 and the value "38" is entered in the ninth position of encrypted data packet 304 to encode the second and third bytes of source data packet 302, respectively. This encryption process continues until all bytes of source data packet 302 have been encrypted.

When all bytes of source data packet 302 have been processed and an encryption value placed in the appropriate position of encrypted data packet 304, the remaining positions

are filled. The remaining positions may be filled with pure random numbers from the sheet of the one-time pad being employed. The positions within the encrypted data packet 304 which do not contain values from the source data packet 302 are used for authentication, verification, and disinformation.

When expanded to include the full character set, the secure encryption mechanism of the present invention possesses the ability to randomly encode each byte of a source data packet in at least 128 different ways. Furthermore, any character of data may be placed in any of the positions within the encrypted data packet. Thus, each character of data may be encrypted in hundreds of thousands of different ways, depending on the length of the encrypted data packet, with each character entirely independent of any other character. There exists no pattern in either the encoding of a character or its position within an encrypted data packet, nor is there any pattern between distinct encrypted data packets. The encoding and position mappings are known only to entities possessing a copy of the one-time pad and knowing which sheet was employed for encryption. No human intervention is required for either the random number generation, encoding, or decoding processes. Once a sheet within the one-time pad has been used, that sheet is never intentionally used again, although theoretically the same sheet may be randomly generated again within another one-time pad.

The feature of randomly ordering encrypted byte within the encrypted data packet is not found in conventional one-time pads, which are simple look-up tables for each character or word placed in order in the encrypted message. Thus, the present invention provides greater security than conventional

one-time pads. Furthermore, the starting location for the position string and arrays may be varied from one-time pad to one-time pad. For example, one one-time pad may begin with the fifth numeral in the position string, while another begins with the fifty-third numeral.

It should be noted that the "arrays" described above are simple constructs used for convenience in describing the invention. Other methods of employing random numbers to encrypt the source data may be employed instead of or in addition to character maps, including XORing the bits of a random number with the bits of the character or word being encrypted.

Referring to **Figure 4**, a high level flowchart for a process of encrypting data in accordance with a preferred embodiment of the present invention is illustrated. The process begins at step **402**, which depicts initiation of the encryption process by a transmitting entity preparing to transmit a source data packet over an unsecured network. The process then passes to step **404**, which illustrates reading a sheet from the one-time pad and, if the one-time pad is equipped with a counter, incrementing the counter.

The process next passes to step **406**, which depicts reading a position indicator from the positions string, and then to step **408**, which illustrates reading the next character to be encrypted from the source data packet. The process passes next to step **410**, which depicts looking up the character to be encrypted in the character map associated with the position identified by the position indicator. The process then passes to step **412**, which illustrates placing the

encrypted character associated in the character map with the character read from the source data packet in the position designated by the position indicator read from the position string.

Once the entire encrypted data packet is filled, the process passes to step 416, which depicts the process becoming idle until another data packet requires encryption. The data packet encrypted by the process described may be securely transmitted over unsecured networks without danger of being compromised.

With reference now to **Figure 5**, a high level flowchart for a process of decoding data in accordance with a preferred embodiment of the present invention is illustrated. The process begins at step **502**, which depicts initiation of the decryption process in response, for example, to receipt of an encrypted data packet. The process then passes to step **504**, which illustrates reading the next available sheet from the one-time pad and, if the optional counter is present, incrementing the counter.

The process next passes to step 506, which depicts reading the first (or next) position in the position string within the one-time pad sheet, and then to step 508, which illustrates reading the encrypted character at the position within the encrypted data packet designated by the position indicator read. The process passes next to step 510, which depicts looking up the encrypted character in the character map associated with the designated position to determine the decoded character. The process then passes to step 512, which illustrates placing the decoded character in the next available position within the decoded data packet.

The process then passes to step 514, which depicts a determination of whether the encrypted data packet has been completely decoded. This determination may be made, for example, based on whether an expected number of characters have been decoded from the encrypted data packet, or on whether a stop character and expected fill characters have been encountered. If further decoding is required, the process returns to step 506 for decryption of additional characters within the encrypted data packet.

A determination of whether the decode was successful may simply involve checking the decoded data packet for a stop character, checking for a known number of characters to be decoded, or may involve looking for an expected authentication or verification character sequence ("watermark" or "signature") within the decoded data packet. When the message has been decoded, the fill characters are checked for authentication and verification purposes.

If the decode was not successful, the process may

optionally proceed to step 518, which illustrates adjusting the one-time pad employed in the decryption process in an attempt to resynchronize the one-time pads employed by the transmitting and receiving entities. This may be achieved, for example, by adjusting the counter value to compensate for the receiving entity being behind the transmitting entity, the most likely source of error in synchronization. If the counter was incremented in the last decryption attempt, the decrypting process may simply be attempted again.

To avoid the potential for synchronization errors in utilizing sheets within the one-time pad, an alternative procedure is to have the decryption process check the fill characters in adjacent sheets for authentication and verification purposes prior to decoding.

Referring again to step 516, if the data packet was successfully decoded, the process proceeds instead to step 520, which depicts the process becoming idle until decryption of a received data packet is once again required.

Referring to **Figure 6**, an electronic checking environment in which secure encryption in accordance with a preferred embodiment of the present invention may be implemented is depicted. The electronic checking environment depicted includes a receiving device 602 located at the merchant's place of business which is connected to a server 604 located at the customer's bank. Receiving device 602 may be connected via communications link 606 to the Internet 608, which is in turn connected via communications link 610 to server 604, such that electronic checks are processed via the Internet. Alternatively, receiving device 602 may be directly connected

to server 604 via communications link 612, which may provide dial-up access or the like.

5 An electronic checkbook 614 is capable of being selectively attached to receiving device 602. The term "electronic checkbook" is used herein to refer to a collection of fixed length randomly encoded data packets, regardless of the medium in which such packets are held, together with the instructions for encrypting. Similarly, the term "electronic check" is used herein to refer to a single fixed length randomly encoded data packet encrypted utilizing the corresponding sheet from a one-time pad. Each electronic check within an electronic checkbook is utilized only once.

10 15 20 25 30 The electronic checks generated by electronic checkbook 614 would contain, in an encrypted data packet, information such as the amount, the payee's account number, and the customer's signature. The signature may comprise a simple password, or may be a fingerprint, retina scan, or any other positive means of identification. The number of bytes required to encode a check's confidential information should be on the order of 100 bytes, although each electronic check may be on the order of a few hundred bytes with the unused bytes filled with additional characters as described above.

25 When an individual first becomes a customer of a bank, or reorders checks, the bank supplies the customer with electronic checkbook 614, with bank routing and account identification associated with the electronic checks. Electronic checkbook 614 may include a reorder form for automatic reorder when the number of remaining checks falls below a certain number. The customer may select a password or

personal identification number (PIN), i.e., signature, to be associated with the electronic checks as is currently done for automated teller machine (ATM) access.

5 The collection of data packets comprising electronic checkbook 614 are contained within a suitable form of electronic memory encased in a hard case or other suitable durable means of protecting the memory. The electronic checkbook 614 may be a simple memory device such as a type of
10 Personal Computer Memory Card International Association (PCMCIA) card capable of being inserted into receiving device 602. Receiving device 602 may thus be equipped with a keyboard and display (not shown) for user interaction and the capability of reading electronic checks from electronic checkbook 614, encrypting transaction information utilizing the associated sheet from a one time pad, and transmitting the encrypted data packet for the transaction while deleting the one-time pad sheet from any local or internal memory in receiving device 602. For additional security, the encryption could occur only within the PCMCIA card. However, this method allows for the possibility of the checkbook owner's password being compromised, which is not the preferred embodiment of the present invention.

25 Alternatively, in the preferred embodiment of the present invention, electronic checkbook 614 could be a relatively simple device allowing for write-only transmission of encrypted data packets. That is, no capability to read its contents would exist. A small keyboard, a small display, and a single port would be required, with electronic checkbook 614 inserted into receiving device 602 when preparing to write an electronic check. Receiving device 602 may be located at the
30

5 merchant's place of business or be connected to a customer's computer for transactions over the Internet. The payee and the amount could be automatically provided by receiving device 602, with the customer entering a password and pressing a write button when the correct payee and amount are displayed. The electronic check would then be written to receiving device 602, which would transmit the electronic check to server 604 for processing.

10 As still another alternative, electronic checkbook 614 may be downloaded into a device possessed by the customer, such as a personal digital assistant (PDA). Electronic checkbook 614 could be downloaded to the customer's PDA at the time the account is opened, with checks replenished without human interaction at ATM's modified to include a port for this purpose. Therefore, check replenishment would be readily available 24 hours a day.

20 25 30 Server 604 located at the customer's bank is connected to a storage device 616 containing the other copy of the one-time pad utilized to encrypt the confidential information within the electronic check and an authorized check list associating electronic checks with sheets of the one-time pad. The electronic checking environment may also include a second server 618 located at the payee's bank connected to Internet 608 by communications link 620, and a third server 622 located at a clearinghouse connected to Internet 608 via communications link 624. In this manner, the electronic checks may be passed among all entities concerned via Internet 608 without generating any paper.

By encrypting the electronic checks using a one-time pad

5

10

in accordance with the present invention, the plain text of at least a portion of the encrypted message--such as the amount, the payee, etc.--may accompany the encrypted electronic check and the encrypted data would still be invulnerable to cryptographic attack. Knowledge of a portion of the message encrypted, even if accompanied by knowledge of the ordering of these portions within the source message, is of no benefit in attempting to break the encrypted message. Thus, authentication and verification codes required to validate the electronic check would remain encrypted in an unbreakable manner.

0
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95

25

An additional level of security may be introduced by varying the starting location used for the position string between electronic checkbooks (i.e., starting with the seventh random number in the string in one electronic checkbook while starting with the thirty first random number in a different electronic checkbook). The responsibility for generating the random numbers for the one-time pad may thus be separated from the responsibility for selecting a starting location within the position string and arrays to be employed by a particular one-time pad, increasing the difficulty of employee theft of the information. An electronic checkbook may be manufactured and filled with one-time sheets by one entity, and programmed with a randomly selected starting location within the position string by a different entity.

30

With reference now to **Figure 7**, a data flow diagram for a process of utilizing electronic checks in accordance with a preferred embodiment of the present invention is depicted. The merchant or payee supplies the merchant's account identification and an amount to the payor through a receiving

device. The electronic check, an encrypted data packet such as described above, is generated by the customer or payor 702 and transmitted to the merchant or payee 704. Merchant 704 appends the merchant's bank routing and account identification numbers to the electronic check, then routes the electronic check to both the payor's bank 706 and the merchant's or payee's own bank 708.

Payor's bank 706 is the only place where the electronic check can be decoded. When payor's bank 706 receives the electronic check, payor's bank 706 decodes the electronic check, verifies and authenticates the check, checks the balance of the payor's account, freezes the amount indicated in the electronic check within the payor's account, and electronically forwards the electronic check, with the appended payee account information, to clearinghouse 710 together with a coded authorization for payment of the indicated amount to the payee.

At the same time, when payee's bank 708 receives the check, payee's bank 708 marks the payee's account as pending receipt of a deposit and forwards the check to clearinghouse 710. Clearinghouse 710 compares the two (encrypted) electronic checks received from payor's bank 706 and payee's bank 708. If they match, clearinghouse subtracts the indicated amount from the clearing account of payor's bank 706, adds the indicated amount to the clearing account of payee's bank 708, notifies payor's bank 706 that the electronic check has been settled, and notifies payee's bank 708 that the electronic check has been settled with the indicated amount placed in the clearing account of payee's bank 708.

5

10

On receipt of the notice from clearinghouse 710, payor's bank 706 subtracts the indicated amount from the payor's account, removes the electronic check from the payor's authorized check list, and notifies the payor 702 that the check has been settled. The payor's electronic checkbook may then remove the used electronic check from the set of available electronic checks. Meanwhile, on receipt of the notice from clearinghouse 710, payee's bank 708 adjusts the payee's account by the indicated amount and notifies payee 704 that the check has been settled.

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

At this point, the transaction is complete. The elapsed time for the transaction could be very short. Bottlenecks will occur primarily from limited bandwidth at the retail counter and within the Internet. Bandwidth problems at the retail counter may be alleviated by using parallel receiving devices.

25

Use of electronic checks over the Internet, directly from a customer's home, would operate in a similar fashion. However, the customer must send a copy of the electronic check to the merchant. Moreover, a number of additional features could be added to the electronic checking system, such as the ability to directly deposit electronic checks to and/or through the customer's electronic checkbook.

30

The electronic checking environment of the present invention would allow the current, paper-based checking system to be electronically emulated, while providing greater security than that available in the current paper process. The ease of understanding and heightened security will facilitate earlier and faster adoption of electronic checking.

5 The current clearinghouse function will persist in an electronic form, and current banking laws, regulations, and procedures may be applied. The present invention also allows paper checks and electronic checks to coexist during a transition period to pure (or majority) electronic banking.

10 Referring to **Figure 8**, a block diagram of a cellular communications global transponder in which a preferred embodiment of the present invention may be implemented is illustrated. Global transponder **802** is a device which automatically returns a data packet containing the latitude and longitude of the location of global transponder **802** in response to receiving a cellular telephone call. The data packets may be transmitted over non-secure, commercial cellular phone circuits such as those provided by the Iridium Project, which provides global cellular communications to and from any spot on earth.

25 Global transponder **802** includes processor **804** connected to memory **806**. The connection may be in the form of a system bus **808**, which is also connected to an external port **810** for programming or communication with other devices. Processor **804** is also connected to cellular modem **812**, which is connected in turn to antenna **814**. Processor **804** and antenna **814** are also both connected to global positioning system (GPS) chip set **816**. Such GPS chip sets are available from a number of commercial sources. GPS chip set **816** preferably returns GPS fix data in the NMEA-0183 ASCII RS232 format. Sensors **818** and switches **820** connected to processor **804** provide sources of data and control, respectively, for global transponder **802**.

30 Global transponder **802** automatically returns a data

5 packet in response to a cellular phone call from a central computer (not shown). The content of the data packet that is returned varies depending on the content of the request packet originating from the central computer. In general, the data packet returned will include GPS latitude and longitude information, and may also include sensor data and/or information regarding the object to which global transponder 802 is attached.

10 When a cellular phone call is received, modem 812 automatically answers and receives the request packet, transmitting the request packet to processor 804. Processor 804 examines the request packet and determines what response packet should be sent. GPS fix data from GPS chip set 816 is stored in memory 806, as is data from sensors 818. Processor 804 extracts the appropriate information from memory 806 for the response packet, forwarding the response packet to modem 812 for transmission. Although the latitude and longitude may be transmitted in approximately 20 digits, the data packets returned may be any fixed length. The data packets could easily be a few hundred bytes long and still be transmitted, in burst mode, in a very short time interval (on the order of one second).

25 There are times when the data packets returned by global transponder 802 must be protected, as in the case of a downed military pilot. Therefore, the one-time pad of the present invention may be employed to encrypt the data packet. A portion of memory 806 may be a microchip containing the one-time pad. When the latitude/longitude of global transponder 802 is required, the central computer dials cellular phone number of global transponder 802 and transmits a request

5 packet comprised of a previously determined pattern of random characters. Processor 804 compares the pattern in the request packet to patterns associated with valid sheets of the one-time pad, copies of which are only in global transponder 802 and the central computer.

10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95
If processor 804 fails to identify a match with patterns associated with the one-time pad, then global transponder 802 simply terminates the cellular telephone connection without returning a data packet. Global transponder 802 may also record the date and time of the attempted contact. On the other hand, if a match to the pattern in the request packet is determined, processor 804 generates a data packet containing the latitude and longitude encrypted using the sheet of the one-time pad which is associated with the pattern from the request packet. This data packet is then returned to the requesting entity (i.e., the central computer).

25 Upon receiving the encrypted data packet, the central computer validates the packet by comparing bytes not containing latitude/longitude information with bytes expected to be returned in response to the request packet. If the packet is valid, the central computer extracts and decodes the encrypted latitude and longitude information.

30 In order to prevent jamming by repeatedly calling the phone number utilized by global transponder 802, it may be desirable to associate a unique phone number with each sheet in the one-time pad. Thus, global transponder 802 would respond to any of the phone numbers associated with sheets in its one-time pad. In addition, for military applications, buttons may be added to allow a downed pilot to indicate

5

his/her physical condition, the state of enemy activity, and whether his/her capture is imminent. The sensors might be used to transmit the pilot's vital signs, such as heart rate. Additionally, functionality may be added to allow the pilot to transmit the information without waiting for an incoming cellular phone call, or to indicate whether the device had fallen into enemy hands.

10

0010-0015
0020-0025
0030-0035
0040-0045
0050-0055
0060-0065
0070-0075
0080-0085
0090-0095
0100-0105
0110-0115
0120-0125
0130-0135
0140-0145
0150-0155
0160-0165
0170-0175
0180-0185
0190-0195
0200-0205
0210-0215
0220-0225
0230-0235
0240-0245
0250-0255
0260-0265
0270-0275
0280-0285
0290-0295
0300-0305
0310-0315
0320-0325
0330-0335
0340-0345
0350-0355
0360-0365
0370-0375
0380-0385
0390-0395
0400-0405
0410-0415
0420-0425
0430-0435
0440-0445
0450-0455
0460-0465
0470-0475
0480-0485
0490-0495
0500-0505
0510-0515
0520-0525
0530-0535
0540-0545
0550-0555
0560-0565
0570-0575
0580-0585
0590-0595
0600-0605
0610-0615
0620-0625
0630-0635
0640-0645
0650-0655
0660-0665
0670-0675
0680-0685
0690-0695
0700-0705
0710-0715
0720-0725
0730-0735
0740-0745
0750-0755
0760-0765
0770-0775
0780-0785
0790-0795
0800-0805
0810-0815
0820-0825
0830-0835
0840-0845
0850-0855
0860-0865
0870-0875
0880-0885
0890-0895
0900-0905
0910-0915
0920-0925
0930-0935
0940-0945
0950-0955
0960-0965
0970-0975
0980-0985
0990-0995
1000-1005
1010-1015
1020-1025
1030-1035
1040-1045
1050-1055
1060-1065
1070-1075
1080-1085
1090-1095
1100-1105
1110-1115
1120-1125
1130-1135
1140-1145
1150-1155
1160-1165
1170-1175
1180-1185
1190-1195
1200-1205
1210-1215
1220-1225
1230-1235
1240-1245
1250-1255
1260-1265
1270-1275
1280-1285
1290-1295
1300-1305
1310-1315
1320-1325
1330-1335
1340-1345
1350-1355
1360-1365
1370-1375
1380-1385
1390-1395
1400-1405
1410-1415
1420-1425
1430-1435
1440-1445
1450-1455
1460-1465
1470-1475
1480-1485
1490-1495
1500-1505
1510-1515
1520-1525
1530-1535
1540-1545
1550-1555
1560-1565
1570-1575
1580-1585
1590-1595
1600-1605
1610-1615
1620-1625
1630-1635
1640-1645
1650-1655
1660-1665
1670-1675
1680-1685
1690-1695
1700-1705
1710-1715
1720-1725
1730-1735
1740-1745
1750-1755
1760-1765
1770-1775
1780-1785
1790-1795
1800-1805
1810-1815
1820-1825
1830-1835
1840-1845
1850-1855
1860-1865
1870-1875
1880-1885
1890-1895
1900-1905
1910-1915
1920-1925
1930-1935
1940-1945
1950-1955
1960-1965
1970-1975
1980-1985
1990-1995
2000-2005
2010-2015
2020-2025
2030-2035
2040-2045
2050-2055
2060-2065
2070-2075
2080-2085
2090-2095
2100-2105
2110-2115
2120-2125
2130-2135
2140-2145
2150-2155
2160-2165
2170-2175
2180-2185
2190-2195
2200-2205
2210-2215
2220-2225
2230-2235
2240-2245
2250-2255
2260-2265
2270-2275
2280-2285
2290-2295
2300-2305
2310-2315
2320-2325
2330-2335
2340-2345
2350-2355
2360-2365
2370-2375
2380-2385
2390-2395
2400-2405
2410-2415
2420-2425
2430-2435
2440-2445
2450-2455
2460-2465
2470-2475
2480-2485
2490-2495
2500-2505
2510-2515
2520-2525
2530-2535
2540-2545
2550-2555
2560-2565
2570-2575
2580-2585
2590-2595
2600-2605
2610-2615
2620-2625
2630-2635
2640-2645
2650-2655
2660-2665
2670-2675
2680-2685
2690-2695
2700-2705
2710-2715
2720-2725
2730-2735
2740-2745
2750-2755
2760-2765
2770-2775
2780-2785
2790-2795
2800-2805
2810-2815
2820-2825
2830-2835
2840-2845
2850-2855
2860-2865
2870-2875
2880-2885
2890-2895
2900-2905
2910-2915
2920-2925
2930-2935
2940-2945
2950-2955
2960-2965
2970-2975
2980-2985
2990-2995
3000-3005
3010-3015
3020-3025
3030-3035
3040-3045
3050-3055
3060-3065
3070-3075
3080-3085
3090-3095
3100-3105
3110-3115
3120-3125
3130-3135
3140-3145
3150-3155
3160-3165
3170-3175
3180-3185
3190-3195
3200-3205
3210-3215
3220-3225
3230-3235
3240-3245
3250-3255
3260-3265
3270-3275
3280-3285
3290-3295
3300-3305
3310-3315
3320-3325
3330-3335
3340-3345
3350-3355
3360-3365
3370-3375
3380-3385
3390-3395
3400-3405
3410-3415
3420-3425
3430-3435
3440-3445
3450-3455
3460-3465
3470-3475
3480-3485
3490-3495
3500-3505
3510-3515
3520-3525
3530-3535
3540-3545
3550-3555
3560-3565
3570-3575
3580-3585
3590-3595
3600-3605
3610-3615
3620-3625
3630-3635
3640-3645
3650-3655
3660-3665
3670-3675
3680-3685
3690-3695
3700-3705
3710-3715
3720-3725
3730-3735
3740-3745
3750-3755
3760-3765
3770-3775
3780-3785
3790-3795
3800-3805
3810-3815
3820-3825
3830-3835
3840-3845
3850-3855
3860-3865
3870-3875
3880-3885
3890-3895
3900-3905
3910-3915
3920-3925
3930-3935
3940-3945
3950-3955
3960-3965
3970-3975
3980-3985
3990-3995
4000-4005
4010-4015
4020-4025
4030-4035
4040-4045
4050-4055
4060-4065
4070-4075
4080-4085
4090-4095
4100-4105
4110-4115
4120-4125
4130-4135
4140-4145
4150-4155
4160-4165
4170-4175
4180-4185
4190-4195
4200-4205
4210-4215
4220-4225
4230-4235
4240-4245
4250-4255
4260-4265
4270-4275
4280-4285
4290-4295
4300-4305
4310-4315
4320-4325
4330-4335
4340-4345
4350-4355
4360-4365
4370-4375
4380-4385
4390-4395
4400-4405
4410-4415
4420-4425
4430-4435
4440-4445
4450-4455
4460-4465
4470-4475
4480-4485
4490-4495
4500-4505
4510-4515
4520-4525
4530-4535
4540-4545
4550-4555
4560-4565
4570-4575
4580-4585
4590-4595
4600-4605
4610-4615
4620-4625
4630-4635
4640-4645
4650-4655
4660-4665
4670-4675
4680-4685
4690-4695
4700-4705
4710-4715
4720-4725
4730-4735
4740-4745
4750-4755
4760-4765
4770-4775
4780-4785
4790-4795
4800-4805
4810-4815
4820-4825
4830-4835
4840-4845
4850-4855
4860-4865
4870-4875
4880-4885
4890-4895
4900-4905
4910-4915
4920-4925
4930-4935
4940-4945
4950-4955
4960-4965
4970-4975
4980-4985
4990-4995
5000-5005
5010-5015
5020-5025
5030-5035
5040-5045
5050-5055
5060-5065
5070-5075
5080-5085
5090-5095
5100-5105
5110-5115
5120-5125
5130-5135
5140-5145
5150-5155
5160-5165
5170-5175
5180-5185
5190-5195
5200-5205
5210-5215
5220-5225
5230-5235
5240-5245
5250-5255
5260-5265
5270-5275
5280-5285
5290-5295
5300-5305
5310-5315
5320-5325
5330-5335
5340-5345
5350-5355
5360-5365
5370-5375
5380-5385
5390-5395
5400-5405
5410-5415
5420-5425
5430-5435
5440-5445
5450-5455
5460-5465
5470-5475
5480-5485
5490-5495
5500-5505
5510-5515
5520-5525
5530-5535
5540-5545
5550-5555
5560-5565
5570-5575
5580-5585
5590-5595
5600-5605
5610-5615
5620-5625
5630-5635
5640-5645
5650-5655
5660-5665
5670-5675
5680-5685
5690-5695
5700-5705
5710-5715
5720-5725
5730-5735
5740-5745
5750-5755
5760-5765
5770-5775
5780-5785
5790-5795
5800-5805
5810-5815
5820-5825
5830-5835
5840-5845
5850-5855
5860-5865
5870-5875
5880-5885
5890-5895
5900-5905
5910-5915
5920-5925
5930-5935
5940-5945
5950-5955
5960-5965
5970-5975
5980-5985
5990-5995
6000-6005
6010-6015
6020-6025
6030-6035
6040-6045
6050-6055
6060-6065
6070-6075
6080-6085
6090-6095
6100-6105
6110-6115
6120-6125
6130-6135
6140-6145
6150-6155
6160-6165
6170-6175
6180-6185
6190-6195
6200-6205
6210-6215
6220-6225
6230-6235
6240-6245
6250-6255
6260-6265
6270-6275
6280-6285
6290-6295
6300-6305
6310-6315
6320-6325
6330-6335
6340-6345
6350-6355
6360-6365
6370-6375
6380-6385
6390-6395
6400-6405
6410-6415
6420-6425
6430-6435
6440-6445
6450-6455
6460-6465
6470-6475
6480-6485
6490-6495
6500-6505
6510-6515
6520-6525
6530-6535
6540-6545
6550-6555
6560-6565
6570-6575
6580-6585
6590-6595
6600-6605
6610-6615
6620-6625
6630-6635
6640-6645
6650-6655
6660-6665
6670-6675
6680-6685
6690-6695
6700-6705
6710-6715
6720-6725
6730-6735
6740-6745
6750-6755
6760-6765
6770-6775
6780-6785
6790-6795
6800-6805
6810-6815
6820-6825
6830-6835
6840-6845
6850-6855
6860-6865
6870-6875
6880-6885
6890-6895
6900-6905
6910-6915
6920-6925
6930-6935
6940-6945
6950-6955
6960-6965
6970-6975
6980-6985
6990-6995
7000-7005
7010-7015
7020-7025
7030-7035
7040-7045
7050-7055
7060-7065
7070-7075
7080-7085
7090-7095
7100-7105
7110-7115
7120-7125
7130-7135
7140-7145
7150-7155
7160-7165
7170-7175
7180-7185
7190-7195
7200-7205
7210-7215
7220-7225
7230-7235
7240-7245
7250-7255
7260-7265
7270-7275
7280-7285
7290-7295
7300-7305
7310-7315
7320-7325
7330-7335
7340-7345
7350-7355
7360-7365
7370-7375
7380-7385
7390-7395
7400-7405
7410-7415
7420-7425
7430-7435
7440-7445
7450-7455
7460-7465
7470-7475
7480-7485
7490-7495
7500-7505
7510-7515
7520-7525
7530-7535
7540-7545
7550-7555
7560-7565
7570-7575
7580-7585
7590-7595
7600-7605
7610-7615
7620-7625
7630-7635
7640-7645
7650-7655
7660-7665
7670-7675
7680-7685
7690-7695
7700-7705
7710-7715
7720-7725
7730-7735
7740-7745
7750-7755
7760-7765
7770-7775
7780-7785
7790-7795
7800-7805
7810-7815
7820-7825
7830-7835
7840-7845
7850-7855
7860-7865
7870-7875
7880-7885
7890-7895
7900-7905
7910-7915
7920-7925
7930-7935
7940-7945
7950-7955
7960-7965
7970-7975
7980-7985
7990-7995
8000-8005
8010-8015
8020-8025
8030-8035
8040-8045
8050-8055
8060-8065
8070-8075
8080-8085
8090-8095
8100-8105
8110-8115
8120-8125
8130-8135
8140-8145
8150-8155
8160-8165
8170-8175
8180-8185
8190-8195
8200-8205
8210-8215
8220-8225
8230-8235
8240-8245
8250-8255
8260-8265
8270-8275
8280-8285
8290-8295
8300-8305
8310-8315
8320-8325
8330-8335
8340-8345
8350-8355
8360-8365
8370-8375
8380-8385
8390-8395
8400-8405
8410-8415
8420-8425
8430-8435
8440-8445
8450-8455
8460-8465
8470-8475
8480-8485
8490-8495
8500-8505
8510-8515
8520-8525
8530-8535
8540-8545
8550-8555
8560-8565
8570-8575
8580-8585
8590-8595
8600-8605
8610-8615
8620-8625
8630-8635
8640-8645
8650-8655
8660-8665
8670-8675
8680-8685
8690-8695
8700-8705
8710-8715
8720-8725
8730-8735
8740-8745
8750-8755
8760-8765
8770-8775
8780-8785
8790-8795
8800-8805
8810-8815
8820-8825
8830-8835
8840-8845
8850-8855
8860-8865
8870-8875
8880-8885
8890-8895
8900-8905
8910-8915
8920-8925
8930-8935
8940-8945
8950-8955
8960-8965
8970-8975
8980-8985
8990-8995
9000-9005
9010-9015
9020-9025
9030-9035
9040-9045
9050-9055
9060-9065
9070-9075
9080-9085
9090-9095
9100-9105
9110-9115
9120-9125
9130-9135
9140-9145
9150-9155
9160-9165
9170-9175
9180-9185
9190-9195
9200-9205
9210-9215
9220-9225
9230-9235
9240-9245
9250-9255
9260-9265
9270-9275
9280-9285
9290-9295
9300-9305
9310-9315
9320-9325
9330-9335
9340-9345
9350-9355
9360-9365
9370-9375
9380-9385
9390-9395
9400-9405
9410-9415
9420-9425
9430-9435
9440-9445
9450-9455
9460-9465
9470-9475
9480-9485
9490-9495
9500-9505
9510-9515
9520-9525
9530-9535
9540-9545
9550-9555
9560-9565
9570-9575
9580-9585
9590-9595
9600-9605
9610-9615
9620-9625
9630-9635
9640-9645
9650-9655
9660-9665
9670-9675
9680-9685
9690-9695
9700-9705
9710-9715
9720-9725
9730-9735
9740-9745
9750-9755
9760-9765
9770-9775
9780-9785
9790-9795
9800-9805
9810-9815
9820-9825
9830-9835
9840-9845
9850-9855
9860-9865
9870-9875
9880-9885
9890-9895
9900-9905
9910-9915
9920-9925
9930-9935
9940-9945
9950-9955
9960-9965
9970-9975
9980-9985
9990-9995
10000-10005
10010-10015
10020-10025
10030-10035
10040-10045
10050-10055
10060-10065
10070-10075
10080-10085
10090-10095
10100-10105
101

5 The vendor may provide a one-time pad to potential customers. For example, a company selling software may provide a one-time pad to a customer setting up an account to order upgrades or new products over the Internet. Alternatively, the user's credit card company may provide a one-time pad for use in conducting transactions over the Internet. Sales orders transmitted over the Internet 904, or at least confidential information within sales orders, are encrypted by user unit 902, and are either decoded by the vendor, if the one-time pad originated from the vendor, or forwarded by the vendor to the credit card company for decoding and payment authorization.

10 Alternatively, the one-time pad may be employed in client-server environments for authentication and verification purposes. In this alternative, a vendor might be able to deliver software customized for a particular environment after receipt of a data packet encrypted using a one-time pad previously sold to the customer.

25 It is important to note that while the present invention has been described in the context of fully functional systems, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally regardless of the particular type of signal bearing media used to actually carry out the distribution. Examples of computer readable media include: recordable type media such as floppy disks and CD-ROMs and transmission type media such as digital and analog communication links.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.